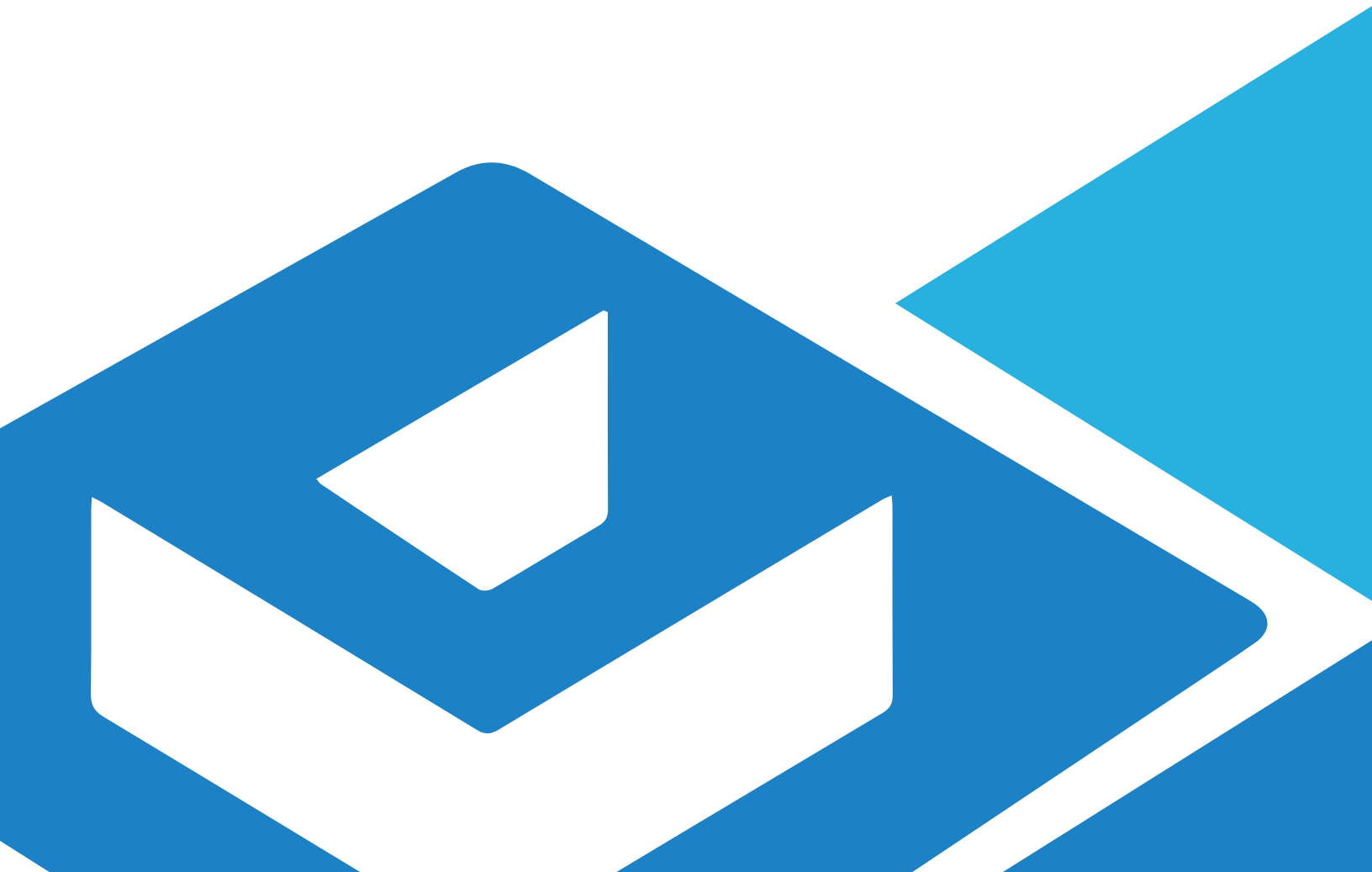
CLEAR CUBE

# Business Continuity During Unexpected Events

WHITE PAPER

April,2020



## Table of Content



CLEARCUBE

# INTRODUCTION

With the recent pandemic, developing a business continuity strategy is imperative to success. Attempts to control the virus are being carried out, and prolonged voluntary or imposed restrictions in travel and cancellations of large gatherings to mitigate its spread have become inevitable. Governments are issuing calls for preparedness as companies continue to modify operations to keep their employees and communities safe.

COVID-19 is driving a cultural change and accelerating the adoption of remote working. All it takes is the right balance of technology, agility, and patience to ensure business continuity in this crisis management scenario.

## ClearCube Solutions

ClearCube enables enterprises to deploy modern digital workspace solutions that facilitate efficient remote work. By combining cloud-ready centralized and virtualized platforms, we give IT departments the ability to remotely deliver any application to practically any device. Employees can instantly work from anywhere, while your enterprise safeguards important information.

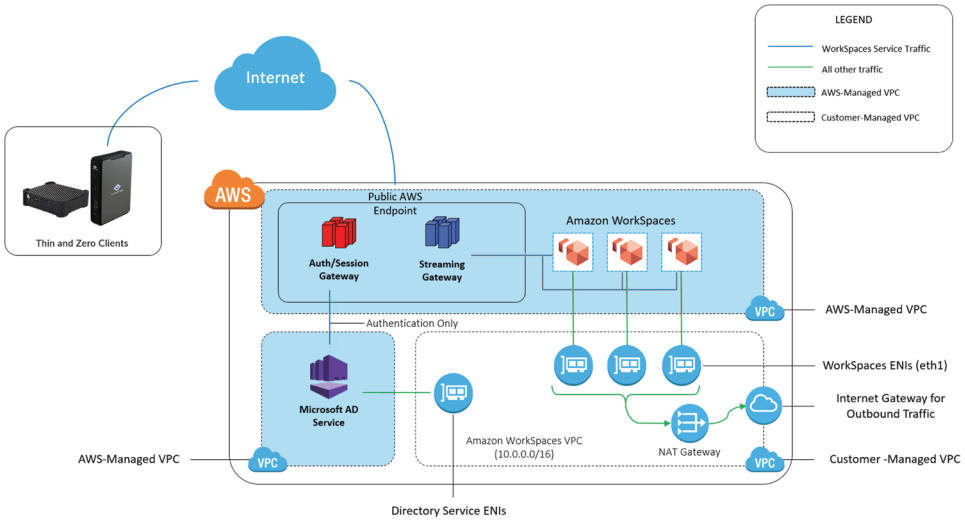
From remote access and VPN to cloud-based solutions, there are multiple tools and technologies you can use to get started.

## Scenario 1: Thin/Zero Clients & Amazon WorkSpaces

Amazon WorkSpaces allows enterprises to provision virtual, cloud-based Windows or Amazon Linux desktops almost instantaneously and quickly scale to provide thousands of desktops. Remote users can access cloud desktops from multiple devices or web browsers with an Internet connection, and administrators need not procure and deploy hardware or install complex software. The platform eliminates administrative tasks associated with managing desktop lifecycle, including provisioning, deploying, maintaining, and recycling desktops.

The following diagram has been taken from the Amazon WorkSpaces (AWS) website. Each Windows and Linux WorkSpace is associated with a virtual private cloud (VPC), and a directory to store and manage data for WorkSpaces and users. Directories are managed via the Directory Service which also authenticates users. Users leverage a client application from a supported device to access WorkSpaces, and, for Windows WorkSpaces, a web browser.

Thin/Zero Clients &
Amazon WorkSpaces



Users can install client applications for devices including Zero Client endpoints. After download, they gain access to the cloud with persistent storage and productivity applications, along with access to files and other resources on the enterprise intranet. Administrators can set up ClearCube Thin and PCoIP Zero Clients for Amazon WorkSpaces environments to facilitate complete PC-in-the-cloud solutions that offer a familiar desktop experience. Enterprises can facilitate employees anywhere, anytime access, while simplifying IT management and the upfront expenses associated with on-premise server-based computing.

If your Zero Client has PCoIP firmware 6.0.0 or newer, your users can directly connect to their WorkSpaces. Your administrator needs to prepare the Teradici PCoIP Connection Manager for Amazon WorkSpaces in case the firmware is between 4.6.0 and 6.0.0. Next, run the Connection Manager authentication appliance in a VPC that hosts your WorkSpaces endpoint. This will broker the connection process and allow for the formation of streaming sessions from WorkSpaces to the clients. As a result, all non-streaming work is offloaded from the clients.

Administrators can install Cloud Desktop OS on any supported Thin Client device. With integrated PCoIP technology , Cloud Desktop OS enables centrally managed and secure Thin Clients and Zero Clients to connect to hosted desktops, cloud-hosted desktops, or centrally hosted applications.

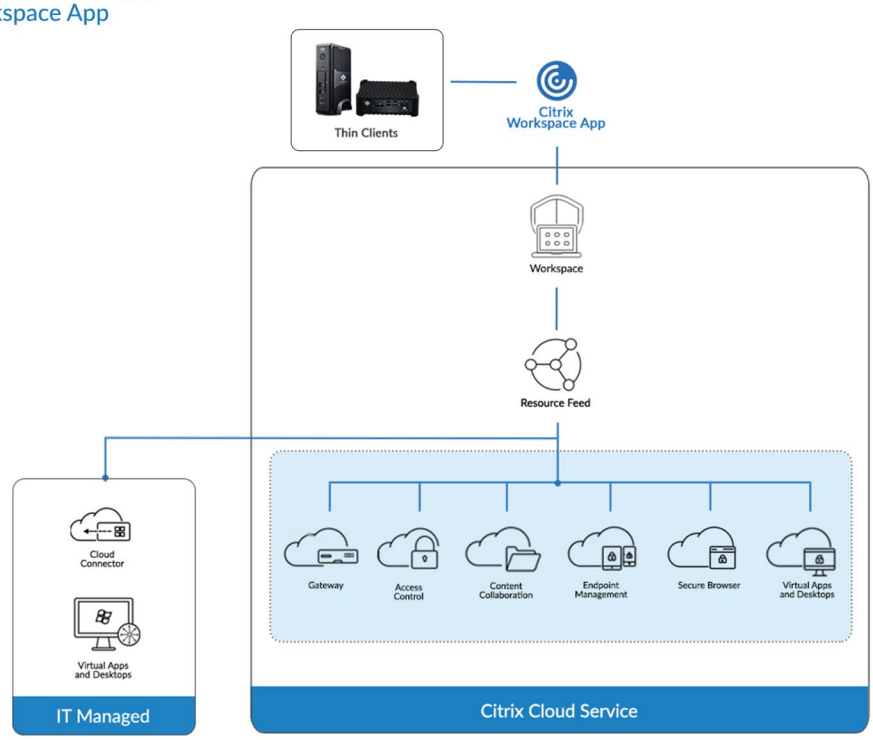
## Scenario 2: Thin Clients & Citrix Workspace App

ClearCube Thin Client devices support Citrix solutions to empower cloud services as well as mobile work styles. These integrated solutions simplify IT deployment, secure business-critical data, feature web/cloud enablement, and allow for work-from-anywhere, anytime, and on any device. Citrix HDX-Ready Thin Clients allow the remote workforce to be innovative and productive while organizations control the balance between access and security of corporate resources. Thin Clients enable task workers, knowledge users, and power users with Citrix Workspace and demonstrate full compliance with Citrix Virtual Apps and Desktops.

Thin Clients connected to the Citrix Workspace enable administrators to deliver cloud-based applications including Microsoft 0ffice 365, email, and web browsers via advanced policies to prevent data loss. An intuitive interface powered by Citrix Workspace enables access to all SaaS and web applications, mobile applications, as well as virtual apps and desktops. Automatic redirection of Internet browsing tasks to a cloud-hosted web browser isolates and safeguards the corporate network.

Refer to the Citrix Workspace App diagram below for a deeper understanding of its architecture.

Thin Clients & Citrix Workspace App



Employees access resources – SaaS apps, Windows apps, Linux apps, web apps, data, and desktops – from several devices. As a result, they require a straightforward and unified experience that allows them to easily gain access to everything they need. Enterprises must make it simple to onboard new devices while ensuring that centralizing security controls has no negative effect on the end user experience.

Workspace is a device-specific environment that gives users a personalized interface for interacting with data and applications. Citrix Workspace app offers capabilities such as access to Virtual Apps and Desktops, SaaS app control, and access to files as well as data through Citrix Content collaboration. Users can choose a Workspace app installed locally on their desktops and mobile devices or utilize local browsers to access a web-based workspace. Irrespective of the selected approach and the preferred device, the overall experience remains familiar while automatically adjusting to the device's form factor and touch-based features. Workspace app integrates multiple engines in a single unified client app, enabling access to different types of application and data resources.

Citrix Workspace app pairs with Citrix Workspace Platform to provide a unified end user experience for single sign-on (SSO) access to Linux, Windows, SaaS/Web and mobile applications. This is implemented via the service feeds in Citrix Workspace. Using a cloud-based management tool, the Citrix Workspace Platform offers a single platform for facilitating a unified administration experience. Inside the WorkSpace Platform, organizations can subscribe numerous cloud services to configure their preferred user workspace experience. Some of the services offered in Workspace Platform include Virtual Apps and Desktops, Secure Browser, Endpoint Management, Content Collaboration, Access Control, and Gateway. These services are managed and updated by Citrix which minimizes deployment and system update effort by administrators.

Citrix Workspace fulfills the expectations of the remote workforce by providing security and mobility capabilities. Unified endpoint management makes it simple to manage mobile devices as well as laptops, desktops, and IoT in a single, secure, central platform. Citrix Workspace also addresses the complexity of managing cloud services alongside existing legacy infrastructure. It functions as a secure digital workspace that streamlines enterprise migration to the cloud by providing the flexibility to opt for any cloud or hybrid infrastructure. Citrix Workspace lets administrators store workloads in the cloud of their choice or in a hybrid scenario. Additionally, organizations can use the solution to monitor, manage, and regulate risk across all their cloud services with advanced security policies and controls.

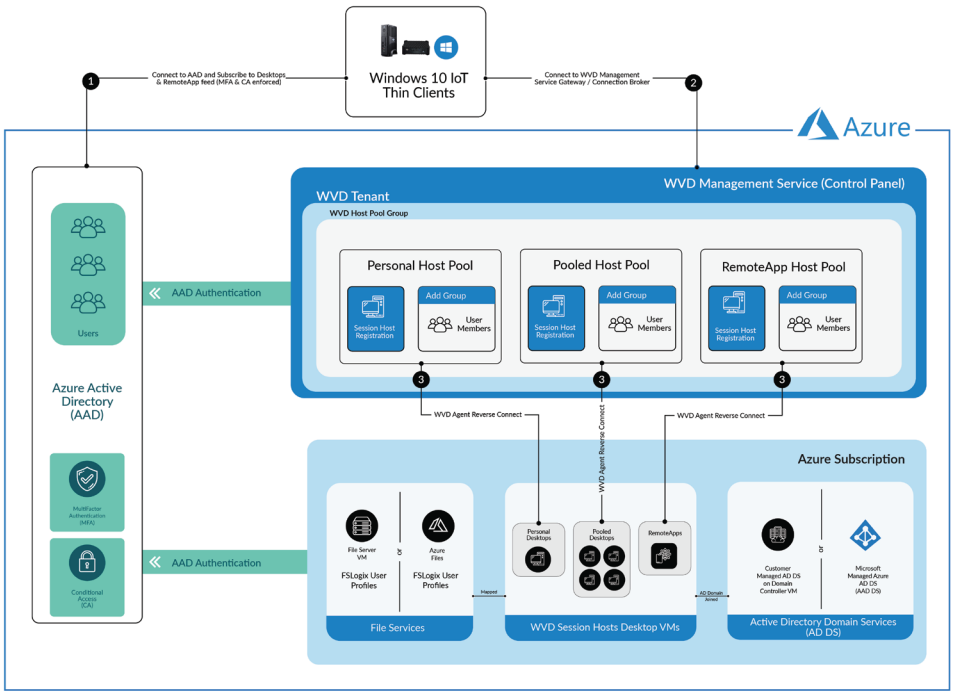
## Scenario 3: WVD & Windows 10 IoT Thin Clients

Microsoft Windows Virtual Desktop (WVD) is a DaaS offering on top of the Microsoft Azure cloud. Infrastructure utilities such as web access, brokering, load balancing, monitoring, and management are prepared for organizations as part of the control plane offering. WVD also provides access to the Windows 10 Enterprise multisession OS which comes optimized for Office 365 ProPlus services, including Teams, Outlook, and OneDrive Files on Demand per machine. The service facilitates remote desktop and remote app experiences without requiring administrators to manage the underlying server infrastructure. It is regarded as a digital workplace solution that eliminates existing barriers to virtual desktops in the cloud for companies. Employees can use WVD to work from home with tools for collaboration, communications, and productivity, while receiving the familiar desktop experience they have in the office.

Windows 10 Enterprise multisession is a Remote Desktop Session Host enabling multiple concurrent interactive sessions, a function which initially only Windows Server could perform. WVD utilizes Azure AD as an identity provider, so administrators can use security controls such as conditional access or multi-factor authentication (MFA). Organizations can have single sign-on (SSO) with Active Directory Federation Services (ADFS), so users will not be prompted to provide credentials when connecting to the VMs.

The following diagram illustrates the components in the Windows Virtual Desktop architecture.

WVD & Windows 10 IoT Thin Clients




Once the host pools are created, users can choose from a number of options to access the virtual desktops:

- Look up the Windows Remote Desktop full client. There are x86 and x64 versions and it supports Windows 7 and Windows 10. After launching the app, the user selects Subscribe and signs in to be able to view the host pool. The Remote Desktop app is also supported on Windows 10 IoT devices including Thin Clients.
- Consider Remote Desktop apps for Android, iOS, and macOS.
- Use an HTML5 browser.

## Thin Client Access

Microsoft WVD incorporates support for ClearCube Windows 10 IoT Enterprise Thin Clients, allowing seamless access to remote sessions. Consider a business scenario in which an organization is looking to replace Azure VMs RDS dedicated for remote sessions with the WVD Azure service. For accessing remote sessions, employees currently use Windows 10 laptops which the company intends to replace with Thin Client devices. Configurations running Windows 10 IoT Enterprise are practical in two cases. They accommodate employees using the web client to launch virtual desktops from the Thin Clients or requiring it to automatically log into virtual desktops upon powering on the devices. This is because Thin Client configurations supporting Windows 10 IoT Enterprise can leverage the WVD 64-bit client and work with Azure AD identity governance for delivering additional security controls.

If an administrator performs central profile management, verify if FSLogix needs the Thin Client endpoint to implement anything. FSLogix is a basic profile management platform used to roam user profiles between different devices. It enables IT to use OneDrive and indexed search in virtual desktops.

## RemoteApp

RemoteApp is an integral part of WVD as it delivers a streaming application experience to a remote client while offering end users the experience of a locally installed application. RemoteApps can be launched from the start menu like a normal application. Those depending on backend data can be co-hosted in the same Azure region to enable fast access for employees on slower Internet links. Also, users with limited compute power or groups that do not have specialized graphics cards can utilize the host to continue running high-demand applications.

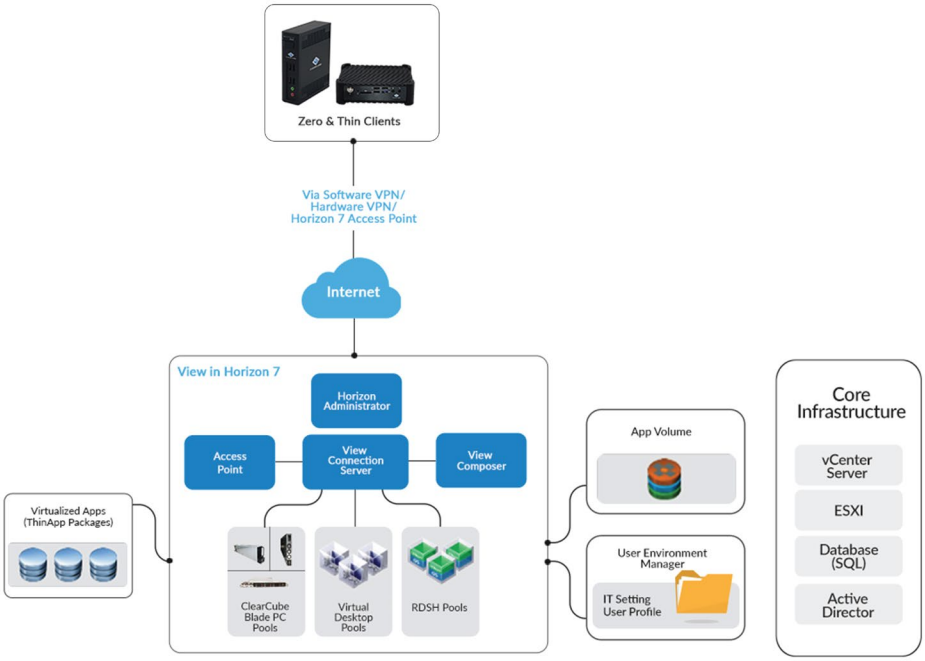
## Scenario 4: VMware Horizon 7 & Thin/Zero Clients

VMware Horizon 7 is a VDI solution that runs VM desktops and applications in a data center and remotely delivers these desktops and applications as a managed service. The technology simplifies and streamlines desktop and application management for IT departments. Administrators can create virtual desktops on demand taking into account user profile and location, and deliver desktops securely as a service from a central location.

Employees can access personalized virtual desktops or remote applications from Thin Client endpoints, company laptops, home PCs, smartphones, or tablets. Horizon 7 also integrates with VMware Workspace ONE to provide a platform for accessing Windows applications and desktops, as well as SaaS, cloud, web, and native mobile applications.

The figure, taken from the VMware website, shows how Horizon components work together to deliver access to virtual desktop pools, RDSH desktop and application pools, and more.

VMware Horizon 7 & Thin/Zero Clients




Employees start Horizon Client to log in to Horizon Connection Server. The server works with Windows Active Directory to facilitate access to remote desktops hosted on a VMware vSphere server, a Microsoft RDS host, or a PC. Horizon Client also facilitates access to published applications on a Microsoft RDS host. Essentially, it is an application that enables users to connect to VMware Horizon virtual desktops from their devices in different locations. Once users enter their credentials in the Client, the application authenticates them by communicating with the View Connection Server. The server then identifies the relevant virtual desktops for users and enables access to them with defined permissions.

Employees can connect to virtual desktops through multiple devices, including Thin Clients and Zero Clients. Thin Clients in VMware Horizon environments represent a flexible method of accessing VDI. A Zero Client forms part of a client-server model, and it comes with an attached keyboard, mouse, and monitor. It integrates a network interface and a user can leverage the device as if they are directly connected to the server. PCoIP Zero Clients are certified for VMware Horizon and can be used in work from home scenarios.

Horizon Administrator manages users and Horizon 7 resources including desktops and applications. With this, administrators can centrally manage thousands of virtual desktops from a single location. Administrators can determine which authentication method best suits the needs of the organization. Access Point in Horizon 7 serves as a secure gateway for external users requiring access to remote desktops and applications from outside the corporate firewall.

If IT departments choose to use a VPN, Horizon 7 fully supports remote access to desktops and applications via a VPN. Horizon 7 fully supports remote access to desktops and applications via a VPN. In this scenario, the VPN software must be set up first and authenticated separately before launching the Horizon Client. The Connection Server handles sessions between users and virtual desktops or published applications. Employees connect to the Connection Server to access their virtual desktops and native, virtual, or RDSH-based applications.

## Managing Desktops, Application, and Blade PC Pools from One Location

Administrators can create pools that consist of one to hundreds or thousands of remote desktops. As a desktop source, IT can use physical machines, VMs, and Windows RDS hosts. When you create a VM as a base image, Horizon 7 can generate a pool of remote desktops from that image. It is also possible to create application pools that provide remote access to applications.

ClearCube PC Blades deliver datacenter-to-desktop compute functionalities for all users in an enterprise. IT organizations can address the demands of task workers, knowledge users, and power users in VDI environments by easily integrating into VMware virtual desktop deployments. VMware Horizon and the Sentral software management suite broker connections between ClearCube PCoIP Zero Clients and Blade PCs. As a result, companies receive VDI-like advantages with ease of management and high availability (HA) in datacenter-friendly solutions.

## Scenario 5: Teradici Cloud Access, PC Blades, and Thin/Zero Clients

ClearCube Blade PCs, workstations, Zero Clients, and Thin Clients offering enterprise-grade security and performance support the Teradici All Access plans. Teradici All Access plans deliver the latest support for PCoIP technology solutions with software, resources, and cloud-ready configurations that optimize and future-proof ClearCube deployments. The plans include secure, modern remoting solutions for users accessing applications and workloads hosted in any public or private cloud.

## Cloud Access Software

Cloud Access is an integral offering in All Access that allows administrators to access hosted Linux and Windows workloads as well as applications anywhere, from any endpoint. The software enables organizations to harness the computing power they need in the cloud while users work from any location on Thin Clients, Zero Clients, tablets, and laptops. It supports on-premises data centers, public clouds, hybrid, and multicloud deployments.

Cloud Access offers high-performance remote visualization features in AWS, Google Cloud, and Azure to deliver dynamic end user experiences for the most graphics-intensive applications and workloads. It enables PCoIP connections between users and remote workstations or desktops that leverage any of several connection models. The solution factors in the number of users, location of users relative to workstations, the plan to integrate public cloud workstations, as well as authentication requirements.

The Cloud Access Manager is a SaaS offering included with Cloud Access subscriptions that allows for cost-effective and highly scalable Cloud Access Software environments. It manages cloud compute hosts and brokers PCoIP connections to remote Linux or Windows workstations. Cloud Access Manager consists of two major components:

**1. Cloud Access Manager Service**

This Teradici service manages Cloud Access deployments.

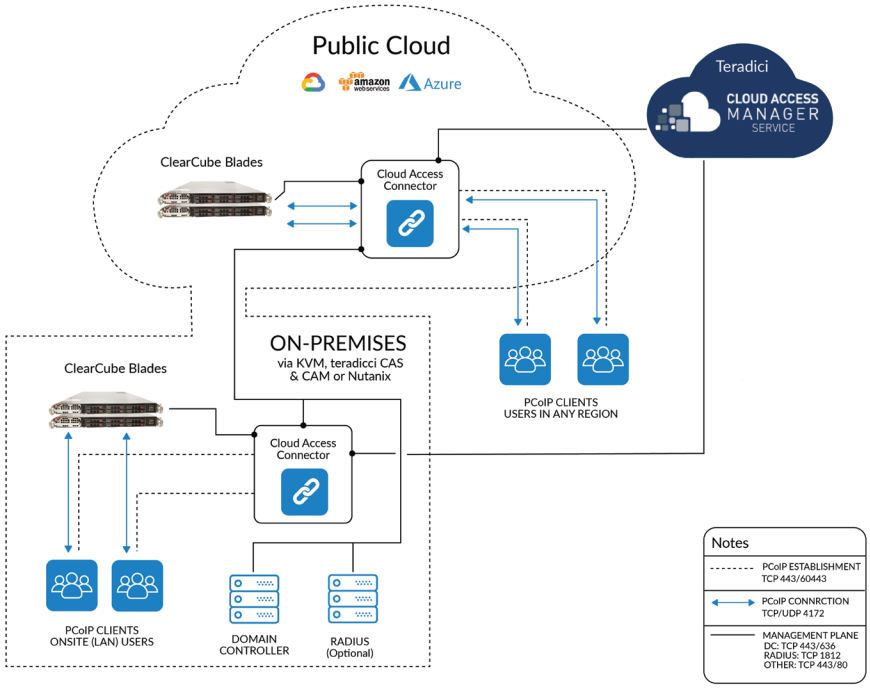
2. **Cloud Access Connector**

This is an access hub deployed in the customer's corporate environment. It facilitates user authentication and machine entitlements of remote desktops or workstations located in Google Cloud, AWS, Microsoft Azure, or on-premises.

With Cloud Access Manager, administrators can install multiple Cloud Access Connectors in several cloud regions, as well as in an on-premises deployment. Apart from managing cloud compute hosts, Cloud Access Manager looks into user entitlement, authentication, and connection brokering in the course of establishing a PCoIP session. Cloud Access Connector allows external users to access remote desktops minus the complexity of endpoint VPNS.

Refer to the diagram below that highlights how the Cloud Access Software works with different technology components.

Teradici Cloud Access,
PC Blades, and Thin/Zero Clients




## Managed Connections For Public Cloud Workstations

Cloud Access Manager integrates support for connections to public cloud workstations. There are two options to implement this. The first is to have administrators provide on-site users with public cloud workstations. Alternatively, you can support employees across different geographic regions with the nearest public cloud workstations by deploying Cloud Access Connector in the desired public cloud. The end user experience is optimized when you opt for public cloud workstations located in close proximity to your remote users.

## Managed Connections For Multicloud Cloud Workstations

Cloud Access Manager supports hybrid multicloud deployments consisting of a combination of on-premises remote workstations (e.g. VMware ESXi, KVM) and public cloud workstations in the preferred public cloud. This can be accomplished by deploying the Cloud Access Connector on-premises and in one or more public clouds. Once again, the end user experience is optimized when you select public cloud workstations located in close proximity to remote users.

## Work From Home With Cloud Access Software

The Cloud Access Software offers different solutions to meet work-from-home demands. It enables remote access to Windows or Linux-based computers, including:

1. Standalone computers or physical workstations (deskside or centralized).
2. Remote workstations that are located in the public cloud.
3. Virtual workstations on VMware ESXi, KVM, or Nutanix AHV hypervisors.
4. Non-graphics virtualized desktops on Vmware ESXi or Nutanix AHV hypervisors.

Using the Cloud Access Software, a software agent is installed on any of the above host variants. The host utilizes PCoIP to communicate with a client device in a remote location over a LAN, WAN, or public internet. The client device is connected to keyboard, mouse, display, and peripheral devices, and is what users interact with.

## Public Cloud Deployment Strategy

Cloud Access Software allows enterprises to deploy public cloud desktops on AWS, Google Cloud, or Azure.

## Cloud Access Software On AWS

This strategy simplifies cloud migration to AWS with virtual workstations. Using PCoIP, Teradici allows for robust and secure visualization of desktops as well as graphically-demanding applications from AWS EC2 G2, G3, and G4, and Elastic GPU instances. Cloud Access Software offers a dynamic and lossless end user experience across different network conditions on desktop and mobile endpoints, including PCoIP Thin and Zero Clients. Data remains secure in the cloud as PCoIP compresses and encrypts the computing experience in the cloud and transmits only pixels to the devices.

## Cloud Access Software on Google Cloud

The Cloud Access Software offers powerful remote virtualization features in Google Cloud virtual workstation instances to accommodate graphics-intensive workloads and applications. Users receive a richand lossless experience across all network conditions on desktop and mobile endpoints, including PCoIP Thin and Zero Clients.

## Cloud Access Software on Azure

Teradici provides secure, remote access to virtual workstations and graphics-intensive applications hosted in Azure. The Cloud Access Software is deployed together with WVD instances across devices including PCoIP Thin and Zero Clients. Furthermore, the platform flexibly supports Windows and Linux operating systems. Data remains secure in Microsoft Azure as PCoIP compresses and encrypts the computing experience in the cloud and transmits only pixels to endpoints. Companies looking to simplify cloud migration to Azure or support a combination of on-premises and hybrid environments can use Cloud Access Software to quicken the process.

## Get Started Today

COVID-19 is changing the way we live and work. At ClearCube, we are committed to supporting our customers with tools and technologies that would help them effectively transition to a work from home environment while maintaining business continuity and operational efficiency. ClearCube has an experienced Sales team available for consultation with customers on how we can further enable our hardware and software solutions to deliver remote work capabilities. We are focusing on addressing the challenges presented by COVID-19 with a strong sense of responsibility and accountability. We are here to support you in every possible way, so please feel free to reach out to our experts for guidance.